REMARKS[1]

In the outstanding Office Action, the Examiner rejected claims 1-4 and 6-9 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,673,319 to Bellare et al. ("Bellare").

By this amendment, Applicants have amended claims 1 and 6-9. Claims 1-4 and 6-9 remain pending.

Applicants respectfully traverse the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 102(b). Bellare does not anticipate claims 1-4 and 6-9.

Claim 1, for example, recites a data storage device including a data storage area and cryptosystem means. The cryptosystem means receives "a first set of keys comprising a plurality of encryption/decryption keys, each of the encryption/decryption keys corresponding to a particular sector and used to encrypt or decrypt that particular sector, for each of the sectors from a device capable of performing data communication with said data storage device." Bellare fails to teach at least the claimed cryptosystem means.

Bellare discloses a set of keys for use in an encryption system, wherein:

> [t]he keys can be derived from some underlying k-bit key K using standard key separation techniques. For example, a_o could be the first k bits of $f_K(0)$, and a_1 could be the first k bits of $f_K(1)$. Bellare, col. 5, lines 43-46.

Bellare, however, does not disclose that any of the keys "correspond[] to a particular sector and [are] used to encrypt or decrypt that particular sector," as recited in amended claim 1 (emphasis added). Bellare cannot anticipate claim 1 for at least this reason.

[1] The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicants decline to automatically subscribe to any statement of characterization in the Office Action.

Bellare also fails to disclose a cryptosystem means that creates encrypted keys wherein the "first and second set of keys are encrypted in a cipher block chaining (CBC) mode by said cryptosystem means using a storage key stored in said data storage device," as recited in claim 1. The Examiner asserts, "Bellare discloses that the first (secret) key (stored in [a] storage device) and an initialization vector are used to generate a CBC message authentication code (MAC) (Column 5 lines 5-21)." Office Action, page 3. The Examiner has thus apparently construed that the first key of Bellare corresponds to Applicants' claimed "storage key." Even if the Examiner's assertion could be considered correct, Bellare teaches:

> [i]t is assumed that the encrypting party and the decrypting party share a pair of secret keys (i.e. a first and a second key). At step 70, the plaintext string is cipher block chained using the first (secret) key and a null initialization vector (IV) to generate a CBC message authentication code (MAC) that is the (entire) last block of ciphertext. At step 72, the plaintext string is again cipher block chained, now using the second (secret) key and the CBC-MAC (generated in step 70) as the initialization vector, to thereby generate an enciphered string. At step 74, the CBC-MAC (generated in step 70) and a portion of the enciphered string (generated in step 72) are then combined to create the ciphertext. Bellare, col. 5, lines 7-19 (emphasis added).

That is, a plaintext string is first cipher block chained using the first key, and the same plaintext string is cipher block chained again using the second key.

Claim 1, however, recites "first and second set of keys are encrypted in a cipher block chaining (CBC) mode by said cryptosystem means using a storage key stored in said data storage device" (emphasis added). Bellare, on the other hand, discloses encrypting, using cipher block chaining, a plaintext string twice, using first and second

keys. Bellare does not provide any disclosure of encrypting a key, and thus also provides no teaching of encrypting "the first and second set of keys," as recited in claim 1.

Bellare also fails to disclose a data storage device including cryptosystem means for creating encrypted keys by using at least "a second set of keys corresponding to integrity-check-value generating keys, the integrity-check-value generating keys being used to check the integrity of data to be stored in at least one of the sectors," as recited in claim 1. Bellare discloses "the enciphered string (generated in step 72) is decrypted by cipher block chaining using the second secret key and the CBC-MAC (generated in step 70) as the initialization vector" (col. 5, line 22-26), wherein the CBC-MAC is "the (entire) last block of ciphertext" (col. 5, line 12). Bellare provides no disclosure, however, of "integrity-check-value generating keys being used to check the integrity of data to be stored in at least one of the sectors," as recited in claim 1.

Because Bellare fails to teach each and every element recited in independent claim 1, Bellare does not anticipate independent claim 1. Accordingly, Applicants respectfully submit that independent claim 1 is allowable over Bellare, and claims 2-4 are allowable at least due to their dependence on claim 1.

Claims 6-9, while of different scope than claim 1, are allowable for at least the reasons given above with respect to claim 1. Accordingly, Applicants respectfully request that the Examiner withdraw the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 102(b).

Please grant any additional extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 18, 2007

By: _____
Darrell D. Kinder, Jr.
Reg. No. 57,460